Substitute for Form 1449/PTO

Information Disclosure Statement By Applicant

(Use as many sheets as necessary)

Application Number	10/527,570
Filing Date:	March 10, 2005
First Named Inventor:	Markus BOCKES
Art Unit:	2136
Examiner Name:	R. Pachura
Attorney Docket Number:	WACHP006

Sheet	1	of	1

U.S. Patent Documents

Examiner Initial	Cite No.	Document No.	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, where Relevant Passages or Relevant Figures Appear
	A	4,405,829	9/1983	Rivest et al.	
	B	4,924,514	5/1990	Matyas et al.	
	C	5,533,126	7/1996	Hazard	
	D	5,675,649	10/1997	Brennan et al.	
	E	2005/0005147	1/2005	Fischer et al.	
	F	6,934,887	8/2005	Baldischweiler	
	G				

Foreign Patent Documents

Examiner Initial	Cite No.	Foreign Patent Document No.	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, where Relevant Passages or Relevant Figures Appear	Translation YES	Translation NO
	H	EP 0 365 065	2/1990	Matyas et al.			
	I	GB 2 270 446	03/1994	Holloway			
	J	DE 689 26 005 T2	10/1996	Matyas et al.		x-abstract	
	K	EP 0 798 892	10/1997	Auerbach et al.			
	L	WO 98/37525	08/1998	Orus et al.		x-abstract	
	M	WO 01/48974	07/2001	Drexler et al.		x-partial	
	N	WO 03/034649	04/2003	Fischer et al.		x-partial	

Non Patent Literature Documents

Examiner Initial	Cite No.	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	O	F. BAO et al., "Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults", *Proc. of 5th Int'l Workshop on Security Protocols*, 1997, pp. 115-124, ISBN 3-540-64040-1
	P	G. ATENIESE et al., "New Multiparty Authentication Services and Key Agreement Protocols," *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 4, April 2000, pp. 628-639
	Q	SUN MICROSYSTEMS, INC., "Java Card™ 2.1.1, Application Programming Interface," 2000, Palo Alto, CA, USA (220 total pages)
	R	V. KLIMA et al., "Attack on Private Signature Keys of the OpenPGP format, PGP™ programs and other applications compatible with OpenPGP," March 2001, pp. 1-20
	S	W. FUNG et al., "Protection of Keys against Modification Attack," *Proc. 2001 IEEE Symposium on Security and Privacy*, May 2001, pp. 26-36
	T	W. RANKL et al.; "Smart Card Handbook," 3rd Ed., John Wiley & Sons, Ltd., pp. 168-175 and 550-556
	U	C. AUMÜLLER et al., "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures," *Proc. 4th Int'l Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002)*, August 2002, pp. 260-275

Examiner Signature		Date Considered	

Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.